E-Safety Policy

Last reviewed:	September 2019
Next review due:	September 2021
Ratified Trust Board:	October 2019

Contents

1. Aims

Our school aims to:

Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

3. Roles and responsibilities

3.1 The governing board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All governors will:

Ensure that they have read and understand this policy
Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 2)

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in school, in particular:

Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school

Working with the headteacher, Head of IT Operations and other staff, as necessary, to address any online safety issues or incidents
Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
Updating and delivering staff training on online safety
Liaising with other agencies and/or external services if necessary
Providing regular reports on online safety in school to the Headteacher and/or governing board

This list is not intended to be exhaustive.

3.4 The Head of IT Operations

The Head of IT Operations is responsible for:

Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
Conducting a full security check and monitoring the school's ICT systems on a real timebasis
Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
Follow recommendations from 3rd parties in terms of cyber security best practices.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

Maintaining an understanding of this policy
Implementing this policy consistently
Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2) and ensuring that students follow the school's terms on acceptable use.
Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 Parents

Parents are expected to:

Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

What are the issues?, UK Safer Internet Centre: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
Hot topics, ChildNet International: http://www.childnet.com/parents-and-carers/hot-topics
Parent factsheet, ChildNet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

4. Educating students about online safety

Students will be taught about online safety as part of the curriculum.

In the **Early Years Foundation Stage** children will be taught:

To use technology safely and respectfully and to know to speak to an adult if they are worried about anything that they have seen on a computer or mobile device.

In **Key Stage 1** children will be taught to:

Use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies.

In **Key Stage 2** children will be taught to:

Use technology safely, respectfully and responsibly; recognise acceptable/unacceptable behaviour; identify a range of ways to report concerns about content and contact.

The KS1 and KS2 statements are lifted from the National Curriculum programmes of study.

In **Key Stage 3**, students will be taught to:

Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
Recognise inappropriate content, contact and conduct, and know how to report concerns

Students in **Key Stage 4 and 5** will be taught:

To understand how changes in technology affect safety, including new ways to protect their online privacy and identity, how to report a range of concerns, the safe use of social media and the internet will also be covered in other subjects where relevant.

The school will use assemblies to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this.

5. Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents on the school website.

Concerns or queries about this policy can be raised with any member of staff.

6. Cyber-bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers and form tutors will discuss cyber-bullying with their tutor groups, and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes Personal Development Time, and other subjects where appropriate.

All staff, governors and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

Cause harm, and/or
Disrupt teaching, and/or
Break any of the school rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

Delete that material, or
Retain it as evidence (of a criminal offence or a breach of school discipline), and/or
Report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

7. Acceptable use of the internet in school

All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet. Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

8. Students using mobile devices in school

This is school specific, and each school will set their own guidelines

Any use of mobile devices in school by students must be in line with the acceptable use agreement.

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device.

9. Staff using devices outside school

Staff members using a work device outside school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use.

Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside school. Any USB devices containing data relating to the school must be encrypted.

If staff have any concerns over the security of their device, they must seek advice from the school's IT Team.

Staff using their own devices must ensure they are running up to date anti-virus software and firewall software for their own protection. The school is not responsible for staff owned devices.

10. How the school will respond to issues of misuse

Where a student misuses the school's ICT systems or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on basic cyber security training, safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The Designated Safeguarding Deputies and his or her Deputies will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety.

13. Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy
Behaviour policy
Staff disciplinary procedures
Data protection policy and privacy notices
Complaints procedure

14. Authentication & Password policy for staff and students

All staff and students will comply with the following password policies:

Staff: Minimum of 10 characters, system will remember the last two used passwords and 5 wrong attempts will lock out the user account for 30 minutes

Students: Minimum of 6 characters, system will remember the last two used passwords and 5 wrong attempts will lock out the user account for 30 minutes

Multi-factor authentication systems will be used where appropriate for both staff and students.

Appendix 1: Students ICT Acceptable Use Agreement

- I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the school network/learning platform with my own username and password.
- I will follow the school's ICT security system and not reveal my passwords to anyone and change them regularly.
- I will only use my school e-mail address.
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher.
- I will not give out any personal information such as name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- Images of students will only be taken, stored and used for school purposes in line with school policy and will not be distributed outside the school network if parents/carers opt out of this by informing the school in writing.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted.

**This is given to parents at the beginning of the admission process. They have to read it to their child, ensure they understand it and then sign to confirm that their child will abide by the rules. This agreement is on the admission booklet and is then also stored in the MIS.

Appendix 2: Acceptable Use Agreement: Staff, Governors and Visitors

Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with, E-safety Coordinator or Headteacher/Head of School or with the Deputy Head Teacher.

- I will only use the school's e-mail/internet/intranet/learning platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Headteacher or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address and social networking identities to students.
- I will only use the approved, secure e-mail system(s) for any school business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorized by the Headteacher or Governing Body.
- I will not install any hardware or software without permission of the school's IT Team.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of staff will only be taken, stored and used for school purposes in line with school policy and will not be distributed outside if staff members opt out of this by informing the Headteacher in writing.
- Images of students will only be taken, stored and used for school purposes in line with school policy and will not be distributed outside the school network if parents/carers opt out of this by informing the school in writing.
- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's E-safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.
- I understand this forms part of the terms and conditions set out in my contract of employment.
- I understand that the current value of laptops and mobile devices brings them below the school's insurance excess levels. Therefore, equipment issued to me will be at my own risk whilst off-site either in transit or at my residence. It is expected that due care and attention will be taken to keep school-issued equipment secure and in good order.

This Acceptable Use Agreement is a summary of our E-safety Policy which is available in full on request.

User Signature:
I agree to follow this code of conduct and to support the safe and secure user of ICT throughout the school.

Signature…… Date…….

Full Name……(printed) Role…….

Appendix 3: Schools, Job Titles & Staff Lists

Notley High School & Braintree Sixth Form

Headteacher: – David Conway
Deputy Headteacher: – Catherine Cusick
E-Safety Coordinator: - Gareth Rose
Designated Safeguarding Lead (DSL): - Christine Wager
Head of IT Operations: - Mark Fuller

The Ramsey Academy

Headteacher: Rob James
Head of School: - Calum Leys
E-Safety Coordinator: - Mike Sharp
Designated Safeguarding Lead (DSL): - Chris Greenslade
Head of IT Operations: - Mark Fuller

Richard De Clare

Head of School: - Karen Riddleston
Deputy Headteacher: - Sam Couttie
E-Safety Coordinator: -
Designated Safeguarding Lead (DSL): - Sam Couttie
Head of IT Operations: - Mark Fuller

Acorn Academy

Headteacher: - Claire Jaques
Assistant Headteachers: - Emma Daniels, Cheryl Noble
E-Safety Coordinator: - Annie Rushant, Claire Jaques
Designated Safeguarding Lead (DSL): - Claire Jaques
Head of IT Operations: - Mark Fuller